Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 15 (2011) 1787 – 1791

Procedia Engineering

www.elsevier.com/locate/procedia

Advanced in Control Engineering and Information Science

A key agreement protocol based-on object identifier for Internet of Things

Yanjiong Wang[a*], Qiaoyan Wen[a]

[a] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing100876, China*

Abstract

By the improvements of R.C. Merkle proposed key agreement protocol, we proposed a unique identifier based on the object identifier key agreement protocol ID-Merkle. The protocol can be widely applied to different objects or items coded system. The ID-Merkle protocol also can be running in an unsafe channel, through cryptography encryption/decryption technology, the protection of the Puzzle was significantly improved. On the one hand, the adjustment of key length can exponentially increase the difficulty an attacker to crack the Puzzle; the other hand, increasing the number of total Puzzles can quadratic increase the amount of time of cracking.

Keywords: internet of things security; key agreement; object identifier; end-to-end security

1. Introduction

In the context of Internet of things (IoT), it is easy to guess the existence or amount of some specified unknown items from a unique identifier of some known object because of its structured coding [1,2] .As a result, some private information of the unknown objects would be disclosed [3]. So that, the identifier (ID)

*Corresponding author. *E-mail address*: wangyanjiong@gmail.com.

This work is supported by National Natural Science Foundation of China (Grant Nos. 60873191, 60903152, 61003286, 60821001) and the Fundamental Research Funds for the Central Universities (Grant No. 2011RC0505).

doi:10.1016/j.proeng.2011.08.332

of object held by the object and the object owner is needed to be protected. In additional, the IDs of object are pre-share secrets between these communication entities in some cases.

In this article we proposed a unique identifier based key agreement scheme by the improvements of R.C. Merkle, which can be adapted to different coding systems. Meanwhile, the protection of each Puzzle has been cryptographically enhanced. The security analysis and performance simulation of ID-Merkle scheme is also given in this paper.

2. Introduction of original Merkle's scheme

In Merkle's scheme [4], there are three important factors of each puzzle:

- A unique puzzle ID
- A random sub-key
- A recognizable text or words

Suppose that Alice and Bob need to agree on a secret key over insecure channel, Alice sends p weak-encrypted puzzles to Bob, after that Bob selects q puzzles to decrypt and returns unique puzzle IDs to Alice.

Because Alice keeps the mapping between puzzle IDs and sub-keys, after she receives these IDs selected by Bob, both Alice and Bob can generate a shared key by these sub-keys. For example, Alice and Bob calculates $K = k_1 \oplus k_2 \oplus \cdots \oplus k_n$.

3. Object Identifier based key agreement scheme

In this section, we describe the scheme of using object identifier to generate the puzzle-key to enhance the safety of each puzzle.

3.1. Length of puzzle-key seed

$h(\cdot)$ is a public hash function, for different input message $m_1 \neq m_2$, the message digest is also different: $h(m_1) \neq h(m_2)$ and the result is L-bits fixed length. For each ID of every object, the L-bits digest is $h(ID)$.

Alice selects a seed length-range $R_a = [r_a - \varepsilon_a, r_a + \varepsilon_a]$ and $r_a > \varepsilon_a > 0$. In the same way, Bob chooses $R_b = [r_b - \varepsilon_b, r_b + \varepsilon_b]$ as his seed length-range, where $r_b > \varepsilon_b > 0$. Furthermore, we let $r_a > r_b$. In order to prevent the length-range set R_a and R_b from empty, we assume that $L > r_a + \varepsilon_a > r_b + \varepsilon_b > r_a - \varepsilon_a > 0$.

Alice and Bob keep $r_a, \varepsilon_a / r_b, \varepsilon_b$ as her/his private parameters.

3.2. Puzzle-key extraction

We denote i as the start index of r-bits length bit string $b_{i,r}$, so that the number of r-bits length seed is $L - r$.

We define $e(\cdot)$ as a public key extraction function, which can generate keys $k_{i,r} = e(b_{i,r})$ to fit the specification of some specified symmetric encrypt/decrypt standard. Meanwhile, we assume that for different bit string b and b', $e(b) \neq e(b')$.

The puzzle-key sets generated by Alice and bob are:

$K_a = \bigcup_{r\in R_a, i\in[0,L-r]} \{k_{i,r}\}$, $K_b = \bigcup_{r\in R_b, i\in[0,L-r]} \{k_{i,r}\}$.

and the sizes of K_a and K_b are:

$|K_a| = \sum_{r\in R_a} (L-r) = (L-r_a)(2\varepsilon_a+1)$, $|K_b| = \sum_{r\in R_b} (L-r) = (L-r_b)(2\varepsilon_b+1)$.

The intersection set of K_a, K_b and its size are:

$$K = K_a \cap K_b = \bigcup_{r\in\{R_a\cap R_b\}, i\in[0,L-r]} \{k_{i,r}\} = \bigcup_{r\in[t_a-\varepsilon_a, t_b+\varepsilon_b], i\in[0,L-r]} \{k_{i,r}\}$$

$$|K| = \sum_{r\in R} (L-r) = [2L-(r_a-\varepsilon_a)-(r_b+\varepsilon_b)]\cdot[(r_b+\varepsilon_b)-(r_a-\varepsilon_a)+1]/2$$

3.3. Alice's and Bob's work

$f_k(\cdot)$, $f_k^{-1}(\cdot)$ is a public encrypt/decrypt function pair, k is the secret key. Alice maintains a plain puzzle set $P = \bigcup_i \{p_i\}$, $i = 1,2,\cdots,N$ ($N >> |K_a|$).

Alice selects $k \in K_a$ and encrypts $|K_a|$ puzzles to generate encrypted puzzle set: $P_a = \bigcup_{k\in K_a, p_k\in P} \{f_k(p_k)\}$. The number of encrypt operations for Alice is $O_a = |P_a| = |K_a|$.

After Bob receives P_a from Alice, he chooses n keys from K_b. For each key k, Bob tries to decrypt each $p \in P_a$. Note that if Bob chooses key from $\overline{K} \cap K_b$, he would not decrypt any puzzle in P_a. In order to increase Bob's efficiency, we suggest that $r_a - \varepsilon_a \le r_b - \varepsilon_b$ and $r_a + \varepsilon_a \ge r_b + \varepsilon_b$. Under these two conditions, we have $K = K_b$. If the recognizable text or words was successful recovered from puzzle, Bob records the ID of this puzzle until he finds out the total n puzzles P_b. The maximum number of decrypt operation for Bob is $O_b \le |P_b| \cdot |K_b| = n \cdot |K_b|$.

4. Security analysis

The goal of attacker Eve is to obtain the key agreed by Alice and Bob, but Eve just can get the encrypted puzzle set P_a and Bob selected sub-key ID set. Furthermore, Eve does not have the digest value of object ID $h(ID)$. Firstly, we denote $R_e = [r_e - \varepsilon_e, r_e + \varepsilon_e]$ as the length of puzzle-key seed selected by Eve. Secondly, Eve should let $R_e \supseteq R_b$, otherwise, it is possible that Eve cannot decrypt some puzzle chosen by Bob. Thirdly, although Eve exactly finds the length $R_e = R_b$, for each $r \in R_e$, she should exhaust 2^r puzzle-key seeds. In that condition, the total number of K_e is:

$$|K_e| = \sum_{r=\min(R_e)}^{\max(R_e)} 2^r = 2^{\min(R_e)} \cdot (2^{\max(R_e)-\min(R_e)+1} - 1) = 2^{\max(R_e)+1} - 2^{\min(R_e)}$$

The maximum number of decrypt operations for Eve is $O_e \le |P_a| \cdot |K_\varepsilon|$, the relation between O_e and R_e is $O(2^n)$.

Consider that if $K_e \cap K = \varnothing$, Eve cannot find out P_b for ever.

5. Security performance simulation

5.1. Puzzle-key extraction

We use DES[6] as the encrypt/decrypt algorithm. Every key used to encrypt puzzle are converted from a bit string $b_{i,r}$ from hash value H, we denote k as one byte of a DES key as follow:

Step A: Calculate $b_{i,r}$ AND 0x7F and assign the result to variable k.

Step B: Left shift k 1 bit (the last of k is parity bit). Let $b_{i,j} = b_{i,j} >> 7$, go to Step A until 8 bytes of DES key have been generated.

For example, if a bit string of a product's hash value is A1138050297B9276B8DD947B36F6E09C$_{16}$, and $i = 32$, $r = 15$, according to the two steps above, the key should be 7A52010101010101$_{16}$.

5.2. The impact of r_e

We assume that $R_e = R_b$ and let $n = 10$, $\varepsilon_a = \varepsilon_b = \varepsilon_e = 0$, $r = r_a = r_b = r_c$, $r \in [7,16]$. t_b, t_e are the time Bob and Eve spent, respectively. The result was shown in Table 1.

Table 1. The simulation result of t_e, t_b, r_b.

r_b	t_b (*ms*)	t_e (ms)	r_b	t_b (*ms*)	t_e (ms)	r_b	t_b (*ms*)	t_e (ms)
7	16	951	11	14	14355	15	16	562762
8	14	1741	12	15	32188	16	15	1975231
9	15	3564	13	15	76195			
10	16	6334	14	15	195422			

We choose $t_e(r_b) = 2^{a \cdot r_b}$ as the fitting function, Table 1 as fitting data. As a result, the coefficient parameter $a = 1.30265$. The data set and $t_e(r_b)$ was shown in Fig. 1.

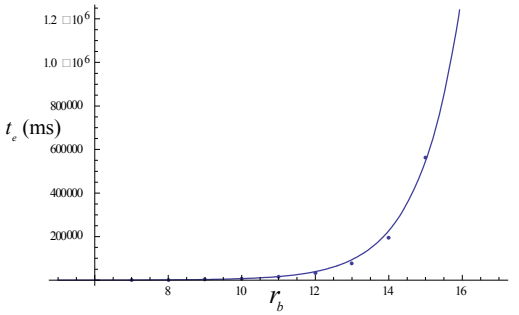

Fig. 1. Fitting formula $t_e(r_b)$ and simulation data set.

5.3. The impact of ε_a

We let $R_e \supseteq R_b$, and $n = 10$, $r_a = r_b \neq r_e$, $\varepsilon_b = \varepsilon_a = 0$, $\varepsilon_a = 3$. The simulation result was shown in Table 2.

Table 2. The simulation result of $|K_e|, t_e, t_b, r_b$.

r_b	t_b (*ms*)	$\mid K_e \mid$	t_e (ms)	r_b	t_b (*ms*)	$\mid K_e \mid$	t_e (ms)
7	10	16256	197859	11	11	32512	585215
8	10	16256	199853	12	11	32512	586321
9	10	16256	193885	13	12	65024	2072039
10	11	32512	589941				

We choose $t_e(\varepsilon_a) = a \cdot \varepsilon_a^{\,2} + b \cdot \varepsilon_a + c$ as the fitting function, Table 2 as fitting data. As a result, the coefficient parameters $a = 2473.25$, $b = 151354$, $c = 77199.5$. The data set and $t_e(\varepsilon_a)$ was shown in Fig. 2.

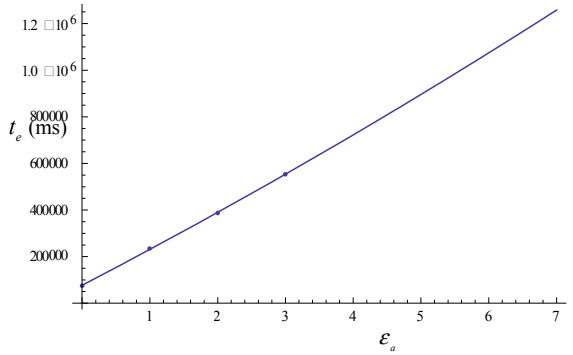

Fig. 2. Fitting formula $t_e(\varepsilon_a)$ and simulation data set.

6. Conclusion

This paper describes an object identifier code based key exchange scheme by the improvement of Merkle's scheme. Comparing with original scheme, the security performance has been improved significantly. This scheme is suitable for different product encoding system. For any two different codes, different keys can be generated by this scheme. This scheme is suitable for asymmetrical computing resources environment.

References

[1] EPCglobal Inc. 860MHz -- 930 MHz Class 1 Radio Frequency (RF) Identification Tag Radio Frequency & Logical Communication Interface Specification. [EB/OL] http://www.gs1.org/epcglobal/standards/specs, 2011.

[2] EPCglobal Inc.13.56 MHz ISM Band Class 1 Radio Frequency (RF) Identification Tag Interface Specification. Avaliable at http://www.gs1.org/epcglobal/standards/specs, 2011.

[3] Chuankun Wu. A Preliminary Investigation on the Security Architecture of the Internet of things (In Chinese). Bulletin of Chinese Academy of Sciences, 2010, 25(4): 411-419

[4] R.C. Merkle. Secure communications over insecure channels. Communications of the ACM, 1978, 21 (4) : 294-299

[5] Piyush Naik, et al. Cryptographic key exchange based on locationing information. Pervasive and Mobile Computing, 2007, 3(1): 15-35.

[6] FIPS 46-2. Data Encryption Standard. Federal Information Processing Standards Publications, 1998

[7] R. Rivest. RFC1321. The MD5 Message-Digest Algorithm. Internet Engineering Task Force. 1992